DEFENSE INFORMATION SYSTEMS AGENCY
CUSTOMER ADVOCACY

July 2002
Volume 2, Number 2

Customer Connection

The Voice for the Warfighter

Inside This Issue

Defense Information Systems Agency
Customer Advocacy
701 South Courthouse Road
Arlington, VA 22204-2199

From The Director

It is our pleasure to present you with the 3rd edition of DISA's *Customer Connection* as part of our ongoing effort to provide up-to-the-minute information on DISA products and services, customer issues and initiatives. This quarter, we are highlighting DISA's Information Assurance Programs. We are proud of the work that our agency does to support DISA's provision of preeminent information assurance to the warfighter, and I believe that these articles will provide understanding of the necessity of information assurance to your mission.

Inside you will find articles from DISA's Customer Advocates that address what they are doing to serve their customer community, as well as an update on the success of the Defense Message System Conference held in April. We have also included an article on the new Encore contract provided by Acquisition Services and a new column "Profile of a DISA Employee" who is working hard to support the agency and ultimately you, the customer. In addition, you will find information on my new Dashboard initiative and an article on NETWARS.

I am honored to have the *Customer Connection* distributed at this year's Customer Partnership Conference 2002. The conference is just another example of DISA's continuing efforts toward becoming a more customer-focused agency. I believe that this event will provide DISA with the feedback we need to better support our customers. In addition, we hope the customers will gain better knowledge of all the products and services DISA has to offer.

Information Assurance Operations: Present and Future

By COL Larry Huffman, USA

During his recent testimony before Congress, the Secretary of Defense outlined six transformation goals for the DoD. Foremost among them was the protection of DoD's information networks from attack, which placed Information Assurance at the forefront of the agenda and certainly in the near future.

The need for this level of DoD-wide visibility has been apparent for some time. *Joint Vision 2020* recognized that: "The United States itself and US forces around the world are subject to information attacks on a continuous basis regardless of the

Information Assurance Operations (Continued)

level and degree of engagement in other domains of operation." The following recent events this year provide proof:

- On April 6, a Russian Internet Protocol (IP) address from the St Petersburg Public Internet Center scanned more than 50,000 DoD hosts searching for vulnerabilities.
- Between January 27 and 28, an entity within the Shenzhen-based Hizhou Metropolitan Area Network scanned more than five million DoD hosts.
- From February 10 to March 10, the NEXCOM Tron, located in Yekaterinburg, Russia, scanned more than two million DoD hosts, once again searching for potential vulnerabilities.

These attempts to compromise DoD information networks are indicators of threats coming from individuals and nation-states around the world. They are extensive, intensive and occur on a 24x7 basis.

Today, the Operations Directorate's Global Network Operations and Security Center (GNOSC) is responsible for directing, managing, controlling, monitoring and protecting essential elements and applications of the Global Information Grid (GIG). This includes:

- Monitoring and correlating network and intrusion events;
- Developing appropriate responses, including protection, detection and reaction;
- Assessing and resolving information security issues in support of the Combatant Commanders and major DoD information processing centers.

The GNOSC consists of the Operations Center and the DoD Computer Emergency Response Team (DoD CERT), both located within the Joint Task Force-Computer Network Operations (JTF-CNO) at DISA Headquarters. This setup affords the opportunity, unique within the DoD, to maintain current visibility of the operational status of the GIG networks, and to defend them.

Recently, the Operations community began several initiatives designed to improve DoD information assurance capabilities. One of these involves a significant upgrade of the DISA Command Center, which includes a major investment in the GNOSC Operations Center. There will be an increase of personnel assigned there, to include supervisors and supporting personnel. The facility will also be upgraded with new tools and visual displays. When these improvements are completed, DISA will have a world- class network operations and security center.

A new organizational capability, called the Combatant Commander Network Operations and Security Capability (CNOSC), is now being piloted. It will be collocated with the Combatant Commander C4I Coordination Centers, and will provide direct support to the Combatant Commanders in maintaining theater network situational awareness, and in providing other network operations support. As a logical extension of the DISA Operations Control Center hierarchy, the CNOSC is expected to be a key player in assisting the Combatant Commanders in improving

The Global Network Operations and Security Center, DISA

The DoD Computer Emergency Response Team, DISA

reporting and responding to network attacks and failures, the completeness of network and information assurance situational awareness, and the overall accuracy of theater information grid operational status.

First steps are now being taken to develop and deploy a critical Enterprise Vulnerability Management System. Threats to DoD systems are increasing with the number of attacks occurring, the speed of propagation of malicious code, and the sophistication of the attack tools being used. It is no longer operationally prudent, or cost-effective, to address vulnerability management in a fragmented approach.

An enterprise-wide system is needed to provide adequate safeguards to critical information systems now and in the future. Such a system will provide near real-time accountability for the installation of vulnerability patches, configuration changes and service packs; and provide dissemination of vulnerabilities to systems administrators.

A pilot project has been initiated to improve the ability to better "see" potential threats originating from the Internet. This program, called the Internet Performance Barometer, involves the use of a web-based corporate Internet monitoring system as a tool to predict potential problems. The goal is to provide an early warning system, or barometer, that may detect attacks such as the recent NIMDA and Code Red events, and allow early preventive measures before a problem crosses the gateway boundaries.

Finally, protection of the deployed JTFs is a priority concern. As DISA provides access to the GIG for the deployed JTFs from the Standardized Tactical Entry Point (STEP) sites, the focus has been on hardening these sites. Actions taken include:

- Installation of a Joint Intrusion Detection System (JIDS) at each of the STEP sites. To date, the JIDS have been installed at sites supporting Central Command (CENTCOM) operations, and are being monitored at the DISA Network Operations and Security Centers.

- Deployment of a robust set of IA tools at the STEP locations, including such capabilities as firewalls, routers and the associated management tools to permit remote management of the firewalls and intrusion detection systems. The final architecture test for these tools is scheduled for May, with installation scheduled for later this year.

Although these efforts add capability, the critical effort of protection lies in the Security Technical Implementation Guides (STIG) the Operations Directorate develops and maintains in cooperation with NSA, GSA, NIST and CIS. These guides, with accompanying checklists and scripts, cover 25 areas including NT systems, UNIX, mainframes, firewalls, databases and wireless, providing specific instructions to systems administrators and network managers on how to secure their systems.

These guides form the basis for DISA Security Policy and are the baseline the Field Security Operations (FSO) Branch uses when testing worldwide DISA and Combatant Commander systems for security readiness. FSO performs more than 2200 reviews annually, which are designed to assist and instruct field unit personnel in the best methods for securing systems and networks. All DISA STIGs and tools are available through the web at http://iase.disa.mil.

While much has been accomplished, much remains to be done. The DISA Operations Directorate is committed to provide IA protection, deterrence, and rapid response to threats against the DoD information infrastructure now and in the future. The goal will always be to ensure that the warfighter has the right information, in the right format, in the right place, at the right time.

For additional information, contact COL Larry Huffman, USA, OP5, (703) 607-6680, DSN 327.

Securing the Warfighter using the Public Key Infrastructure

By Barbara Keller, API1

Public Key Infrastructure (PKI) – in brief

Public Key Infrastructure (PKI) is a non-forgeable electronic identity credential used for all sorts of functions in cyberspace. As part of its Defense-in-Depth strategy, the DoD is deploying PKI to enable information security services on both the NIPRNet and SIPRNet. The PKI produces, distributes, and manages public key (digital) certificates. It associates users with electronic public keys, issuing these keys in digital certificates along with a related private key. It provides key management services, such as recovering lost keys, revoking keys, and supplying lists of revoked keys for use by applications. Users of PKI services include people and applications, and are used with public key-enabled applications to apply security measures, such as encryption or digital signatures. Users can also use their certificates for authentication during workstation logon, or connecting to public key-enabled web servers.

Initially, keys and certificates were issued on low security floppy disks. In 2000, the Deputy Secretary of Defense issued a memorandum mandating the Common Access Card as the primary token for the PKI. So far, more than 620,000 certificates have been issued on floppy disks and the Common Access Card - and the number is increasing by more than 7,000 a day.

How can I use the PKI?

some examples…

- Gaining remote access to your office network using your PKI credential instead of using a user ID and password
- Keeping business transactions between your computer and a web server hidden from eavesdroppers
- Proving that you completed a business transaction, for example approving an invoice payment
- Providing assurance that an email message was not changed in transmission
- Ensuring that the software that you downloaded from the network is authentic and is unmodified

MGS

Medium Grade Service (MGS) is a set of Commercial Off-The-Shelf (COTS) email products, that use the DoD Public Key Infrastructure. MGS provides secure, interoperable messaging in an open, multi-vendor environment.

The DoD PKI is based on a policy jointly approved by all the Services and Agencies and universally recognized technical standards and protocols. As a result, public key-enabled applications can communicate sensitive, unclassified information securely over shared networks, automate sensitive processing previously done offline, separate communities of interest on classified networks, and facilitate the use of the Internet for business. One of the first users of the PKI in the DoD was DISA's Medium Grade Services (MGS), which demonstrated the use of PKI technology in protected email.

CENTRAL COMMMAND (CENTCOM) Implements PKI

In 2000, the Central Command (CENTCOM) asked DISA to implement a MGS pilot for the Internal Look exercise, which involved deploying secure e-mail for about 40 CENTCOM users. CENTCOM's goal was to protect sensitive e-mail from exposure to unauthorized persons using encryption, and to allow users to confirm that e-mail messages received were actually sent by the indicated sender and no one else using digital signatures.

CENTCOM judged the use of secure e-mail a success, and decided to extend the results to their headquarters domain. As a first step, another pilot involving MGS and about 50 headquarters personnel was planned to support the "Bright Star" exercise that was held in October – November 2001. A DISA MGS team deployed to prepare for the exercise during the first week in September.

CENTCOM

United States Central Command is a headquarters element - it has no resident warfighting personnel. All four Armed Services provide USCENTCOM with a component command, which, along with a joint special operations component, make up USCENTCOM's primary warfighting and engagement organizations.

In the aftermath of September 11, CENTCOM asked DISA to plan and roll out MGS across the entire headquarters. DISA responded immediately by first helping CENTCOM develop a plan. The MGS team advised CENTCOM on whether certificates should be issued on floppy disks or the more secure Common Access Cards, which were just beginning to be issued in quantity.

CENTCOM chose the Common Access Card. As the implementation progressed, the DISA MGS team helped to piece together usable computer resources out of existing equipment. The team helped CENTCOM identify replacement workstation hardware platforms, and compatible software that would enhance security.

At the time, CENTCOM headquarters RAPIDS workstations had not been upgraded so that Common Access Cards could be issued. The MGS team negotiated with the Defense Manpower Data Center (DMDC) to move CENTCOM higher on the priority list, and made arrangements with the Air Force PKI Special Projects Office (SPO) for the first use of their new mobile RAPIDS mass issuance van to speed CAC deployment. CENTCOM began to issue Common Access Cards beginning in the fall of 2001.

As new users were registered, the MGS team worked with CENTCOM's contractors to train users in their Common Access Cards and email security features. By the time the PKI deployment wrapped up in mid-March 2002, more than 2,700 users had Common Access Cards with digital certificates and private keys, and were using these tools to secure e-mail correspondence.

Bright Star

Bright Star is rooted in Egypt's signing of the 1979 Camp David Peace Accord. Afterwards, the US military began to train side-by-side with the Egyptian military in the Egyptian desert. This small unit training has evolved into a Joint/ Combined Coalition computer-aided, command post exercise and a tactical field training exercise involving 10 countries and more than 70,000 troops every two years.

In a short time, DISA has helped CENTCOM implement and put into daily use important security tools that enhance mission security. Although CENTCOM's use of PKI services is still in its infancy, they are rapidly gaining an understanding of the power of the technology and developing a vision for its future use. They are already planning to use PKI services to secure other applications, such as the virtual private networks.

The DISA PKI Team's mission is to provide tools and services for use in improving information systems security across DoD. Public key technologies can provide a strong security foundation for automating manual business processes, and securing applications in a wide range of business areas, such as financial, contracting, personnel, and logistics. The PKI Team can help you determine if using the PKI is right for your needs.

For additional information, contact the DISA PKI Team at (703) 882-1631, DSN 381, or by email at PKI@ncr.disa.mil. POC is Barbara Keller, API1, (703) 882-1637, DSN 381.

Delighting Our Department of Defense and Federal Agencies

by JoMarie Coburn, CA4

DISA's Customer Advocacy Directorate is devoted to putting the customer first. To do this, each division within the organization makes sure that their assigned military service or agency is taken care of. The Agency Support Office (CA4) is responsible for the DoD and all Federal Government agencies.

The goal is to ensure that agencies that come to CA4 for support are able to perform their missions. Unfortunately, even in the best of circumstances, problems and issues arise and Customer Advocates are there to ensure that concerns are heard and sent to the proper division, so that a timely and accurate solution can be expedited.

The DoD and Federal Agency Customer Advocates make sure customers are aware of the status of requirements submitted to DISA. These requirements range from obtaining a Point-to-Point Protocol (PPP) account to requests for how to establish a Community of Interest Network (COIN). As advocates for the customer, CA4 follows up on issues to determine that solutions were met with customer approval. CA4 also actively engages with the customer and internal DISA staff to evaluate long range options and opportunities to provide better support.

An important function within CA4 is the support of high-level visits to DISA. Customers and representatives of the nation's allied countries are given executive briefings on DISA products and services, as well as the opportunity to tour the Global Network Operations and Security Center (GNOSC). CA4 also acts as the liaison between DISA and DoD and Federal agencies by coordinating meetings, and sitting in on working groups that discuss techniques to better serve DISA customers.

Customer advocates in CA4 are implementing various initiatives that will keep DISA abreast of customer needs and requirements. The CA4 team also keeps customer profiles that are continuously updated so that all team members know the customers' missions, agency responsibilities, organizational structures and historic use of DISA services.

For additional information, contact JoMarie Coburn, CA4, (703) 882-0711, DSN 381.

Nature of Simple Network Management Protocol (SNMP) Vulnerability by Tom Lam, TS1

Scandinavian researchers discovered that there are numerous vulnerabilities in several implementations of the Simple Network Management Protocol (SNMP). This protocol is implemented by nearly every networking device, and is used extensively throughout both the Internet and DoD networks.

SNMP: A protocol governing network management and the monitoring of network devices and their functions.

The most recently discovered vulnerabilities may cause a variety of problems and degraded states including unstable behavior, corrupt memory, unauthorized privilege elevation, root access, and denial of service. Due to the widespread nature of this problem, it is vital that DoD and other system administrators keep up to date on the latest security patches.

A Government-Wide Effort

The SNMP vulnerability has government-wide focus. Even before the initial Computer Emergency Response Team (CERT) announcement, DISA proactively attacked the problem. The Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, provides SNMP oversight and direction; the US Space Command (USSPACECOM) is the focal point for coordinating and monitoring all SNMP activities within DoD.

The Joint Task Force-Computer Network Operations (JTF-CNO), a subordinate command of the U.S. Air Force's Space Command (USSPACECOM), is the day-to-day operational arm. DISA, the technical leader in DoD communications, is the focal point for SNMP alerting, testing, and operational procedures. SNMP vulnerability also has significant attention from several Federal civilian agencies. The White House Special Advisor for Cyber Security, Richard Clarke, established the Cyber Inter-agency Working Group to manage the Federal and Industry response to the SNMP vulnerability.

DISA Strategy and Progress

DISA developed a successful strategy to solve the problem. Army Major General J. David Bryan, Vice Director of DISA and Commander of the JTF-CNO, established the DISA SNMP Vulnerability Task Force. Chaired by Dr. Jeremy Kaplan, Director of Technical Integration Services, the Task Force includes representatives from all DISA Directorates. The Task Force has formulated a four-pronged strategy for managing the SNMP vulnerability with respect to DISA assets and developed applications: Alert, Block, Harden, and Detect.

Alert

The Task Force established a Technical Assessment Working Group (TAWG), headed by the DoD CERT, to develop Alerts, Bulletins and Technical Advisories to Combatant Commanders, the military services, and agencies regarding the SNMP vulnerability. To date, DoD CERT issued three SNMP Information Assurance Vulnerability Alerts (IAVA) and three Technical Advisories.

Alert	Tech Advisory
2002-A-SNMP-001	2002-T-SNMP-001
2002-A-SNMP-002	2002-T-SNMP-002
2002-A-SNMP-003	2002-T-SNMP-003

In conjunction with this effort, the Joint Interoperability Test Command (JITC) developed a patch test methodology and patch information sharing website and database. The JITC test methodology provides scripts and documentation to simplify the use of the OULO University PROTOS test suite, as well as documenta-

Members of the Department of Defense Computer Emergency Response Team, Defense Information Systems Agency monitor the DoD networks for intrusion by unauthorized users.

tion on the use of the JITC test methodology. The patch information website and database is an information sharing mechanism that allows DoD components to share test results for vulnerability testing of vendor delivered patches.

Block

Blocking is comprised of Access Control Lists (ACL) applied at various routers to prevent transmission of SNMP over the Defense Information System Network (DISN), except as required. In accordance with this strategy, ACLs were applied at all inbound interfaces from the Internet to NIPRNet and the Gigabit Switch Router (GSR) network on six SNMP ports, as well as at all authorized backdoors to the Internet. In addition, SNMP traffic was restricted to identified Internet Protocol (IP) addresses at the Defense Enterprise Computing Centers (DECC), DISANet and DTIC enclaves.

Harden

Network Services began patch testing and application to the GSR routers and the Defense Asynchronous Transmission Mode System (DATMS). To date, the GSR network is completely patched. Updated patches from Cisco are in regression testing now, and will begin to be rolled out to CONUS NIPRNet shortly. In March, the foregoing SNMP IAVAs and patch information database web site (http://199.208.204.125/snmp) initiated patch implementation.

Detect

Existing detection systems are monitoring the NIPRNet boundary, and there are additional efforts underway to capture SNMP attempts for analysis.

The Long Term Solution

DISA and the DoD are making great strides in patching current SNMP-managed devices against problems discovered by the PROTOS test suite. In doing so, one of the lessons learned is that the current approach is unlikely to provide an affordable or successful solution to SNMP and other so-called Abstract Syntax Notation version 1 (ASN.1) protocol vulnerabilities in the mid and long term. A successful long-term approach will likely involve the following:

- Efforts in standards.
- Understanding how to write and promote the writing of secure SNMP applications.
- Development and distribution of commercial freeware for decoding Basic Encoding Rules (BER) (and other encoding rules) of SNMP and other protocols.

It may also involve influencing developers of networking devices to properly implement and test their systems for known vulnerabilities and common exploitations. DISA, with its DoD-wide charters in information technology standards and testing, its charter in information security, and its expertise in applications engineering could take the lead in developing a program in this arena.

For additional information, contact Tom Lam, TS1, (703) 882-1744, DSN 381, or Mitch Komaroff, TS1, (703) 882-1739, DSN 381.

Defense Message System (DMS) Conference

By Paula Sendish, APM

Approximately 1100 representatives from the military services, Combatant Commanders, Joint Staff, Office of the Secretary of Defense (OSD), government agencies, and industry participated in the 6th Defense Message System Conference in San Diego, CA, April 7-10.

The focus of the conference was to provide DMS customers an update on the latest program developments and products. Keynote speakers included Frank Criste, from OASD (C3I), Air Force Brigadier General Bernard "Bernie" Skoch, DISA's Principal Director for Customer Advocacy, and Diann McCoy, Principal Director for Applications Engineering.

The hands-on DMS laboratory provided users and system administrators with the unique opportunity to receive training in conjunction with interacting with developers and engineers. military services and agency Program Managers (PMs), and the Joint Staff/Combatant Commander representatives held breakout sessions to cover unique organizational issues.

The exhibit hall displayed DMS-related products and capabilities from 18 DMS vendors, and the DISA and Navy DMS PMOs. Sessions called "Ask the Expert" gave attendees the opportunity to meet with DMS subject matter experts and address individual needs and concerns. In addition, numerous ad hoc meetings allowed participants to address key issues.

The next DMS Conference is scheduled for May 2003 and will be held in Nashville, TN. Details will be provided this October.

For additional information, contact Paula Sendish, APM, (703) 882-1647, DSN 381.

Focus on our Service Customers

By Elisabeth Cordray, CA3

The Principal Directorate for Customer Advocacy (CA) seeks to improve DISA's services to the customers. DISA field offices have served as the front line of support to the Combatant Commanders.

Following a similar model, CA assigned a customer advocate to each group to represent that customer's view within DISA. One of the divisions within CA is the Military Department Support Office (CA3), which supports DISA's three largest customers: the Army, Navy, and Air Force.

Although each customer is unique, the basic functions of CA3 are similar. Activities range from acting as an information portal, to articulating important customer issues for internal work prioritization, to coordinating restoration of network services.

Customer: U. S. Army

The Army Customer Advocate (CA) ensures that DISA understands the Army's strategic direction and priorities. After the September 11 attack, the Army Customer Advocate was engaged with the C3I senior leadership within the DoD and the Army to ensure continuity of operations (COOP) with DoD and continuity of government (COG) at the highest levels were maintained.

The CA assisted with the development of requirements, and facilitated the implementation of plans and support operations that eventually led to the development of the "virtual Pentagon" program. Understanding the needs of customers involved and integrating them with other programs, projects, products, and services already provided by DISA, expedited the achievement of the desired results.

The CA has worked closely with Army Materiel Command on the Wholesale Logistics Modernization Program (WLMP) to ensure its success. The CA assisted the Communications-Electronics Command (CECOM) Program Manager (PM) and the contractor in identifying contractual issues regarding the procurement of Defense Information System Network (DISN) services for a commercial service provider; the development and tracking of the requests for communications services; the generation of memorandums of agreement for DISN status information; and shared use of space within a DISA operated facility.

Operating under the "knowledge is power" concept, the CA is educating the senior leaders of the Signal Corps to maximize their opportunities for success. The CA conducted DISA information briefings at the Army Signal Corps Pre-Command Course and Director of Information Management (DOIM) Course. The briefings were well received, and will be extended to the Army Command and General Staff Officer in the next academic year.

Customer: U.S. NAVY

The Navy Customer Advocate supports the Navy and Marine Corps customers by providing services ranging from expediting DISN services to deployed naval units operating in Southwest Asia, to coordinating the reconstitution of C2 services, and supporting the relocation of the Navy elements after the September 11 attack.

Working closely with the Navy's Naval Network Operations Command (NNOC) and the Marine Corps Information Technology Network Operations Center (MITNOC), the CA has developed procedures to monitor new circuit provisioning actions and track systemic circuit outages or degraded performance.

When the Marine Corps Chemical Biological Incident Response

Force (CBIRF) relocated to the National Capital Region, the installation of a critical SIPRNet circuit was delayed due to a local labor strike and coordination difficulties with the installation Information Technology (IT) manager. The CA coordinated the installation schedule, and assisted in the resolution of technical issues to complete the SIPRNet installation in time to support the Presidential Inauguration.

Future initiatives by the Navy Customer Advocate include a Professional Military Education Class highlighting DISA and the management of the Global Information Grid for IT professionals.

Customer: U.S. Air Force

The Air Force Customer Advocate opened and enhanced communications to synchronize DISA's efforts to support implementation of Air Force Vision 2020. DISA's support will be critical to the Air Force's achieving its goals of Global Vigilance, Reach, and Power.

At the strategic level, the CA organized and supported meetings between DISA, the Secretary of the Air Force, Undersecretary of the AF for Manpower and Reserve Affairs, 8th AF/CC, AF/CIO, AF/SC, and ESC/CC. More than "Chamber of Commerce" presentations, these meetings included dialogue and exchanges of detailed information that help DISA improve its focus on meeting the Air Force's needs. The CA has also been actively engaged in building working level relations with Air Force organizations to close Air Force Action Items in the Director's 2002 500 Day Action Plan.

At the operational level, the CA facilitated a meeting between DISA's GNOSC, Network Services, the Air Force Network Operations Center, and the Air Staff to establish a plan to improve customer visibility into the health of its communications network. This meeting laid the groundwork to synchronize and formalize escalation procedures between network operations organizations, ensuring that resolution of network problems are prioritized based on the impact to customer missions.

The CA also worked with directorates within DISA to develop a community of interest network for the Joint Strike Fighter Program Office, enabling data sharing across geographically distributed support elements of this high-visibility/high-dollar acquisition effort.

At the tactical level, the CA engaged DISA to respond to "immediate" Air Force issues. These actions included the restoration of network services and resolution of software problems, expediting NIPRNet bandwidth access in support of an imminent Air Force test, and developing alternate phased solutions to meet implementation of time-critical VIP communications.

DISA has more than 8,000 employees ready to provide the best value, most secure, and reliable IT products and services in the world. Customer Advocacy exists to help DISA maintain the focus on the customers. Customer Advocacy's goal is to continue to improve communications between DISA and the Army, Navy and Air Force.

For additional information, contact Elisabeth Cordray, CA3, (703) 882-0928, DSN 381.

Director's Dashboard: Providing the Daily Pulse of the "The Customers' Perspective of DISA" by Jose Finn, CAI

The Director's Dashboard is used to gauge the daily pulse of "the customers' perspective of DISA." It provides the Director, Vice Director, Senior Executive Account Managers (SEAM), and Customer Advocates with an immediate, at-a-glance view of the status of various customer related metrics and issues.

The Principal Directorate for Customer Advocacy is responsible for the development, use, and maintenance of the Director's Dashboard, which provides near real-time information concerning the overall agency's performance from the customers' perspective.

A true web-based tool, the dashboard gives the Director a daily overall status of customer issues by using color-coding based on pre-defined criteria assigned by respective Customer Advocates/ SEAMs for each primary customer issue. The first page of the dashboard visually reports customer issues at the strategic high level. Related and more detailed information is made instantly available by the dashboard's drilldown capability, which lets the Director review pertinent details and escalation information for any given issue by clicking a mouse.

The Director's Dashboard is another example of DISA's commitment to its customer-focused business model. It has proven to be an invaluable tool in advocating customers' needs, priorities and concerns to the Director and staff, facilitating DISA strategies and solutions that provide customers with the information superiority they need to accomplish their missions.

For additional information, contact Jose Finn, CA1, (703) 882-0509, DSN 381.

Customer: Chief Information Officer (CIO), Office of the Secretary of Defense (OSD) by Joe Re, CA2

Based on a review conducted by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence [ASD(C3I)], the OSD Chief Information Officer (CIO) organization was created.

The review found that 15 OSD components manage their own sub-networks; there was no centralized management; there was little configuration management; and that there was inadequate network and security architecture. OSD came to DISA to identify what support could be provided. The Principal Director for Customer Advocacy, in conjunction with the Joint Staff Support Center (JSSC), determined that DISA could provide technical assistance with plans and policy, network and security architecture, technology consultation, and training.

Through the OSD customer advocate interface with OSD, DISA has provided OSD CIO support in security by scheduling and conducting Security Readiness Reviews (SRR); providing Intrusion Detection System (IDS) product evaluation; assisting with identifying activities on OSD's domain through the NIPRNet Connection Approval Process (CAP) review; supporting the Defense Information System Network (DISN) Security Accreditation Working Group (DSAWG), the Global Information Grid (GIG) Waiver Process for unclassified Remote Access Service (dial-up) and a wireless pilot program (Blackberry); and continuing security training for both current and future scheduling and attendance.

DISA has also provided enterprise and standard based architecture consultation support, as well as some policy and plans support on a limited basis.

Our customer advocate partnership with the OSD CIO organization has been a positive step to help them develop a plan to centralize OSD component IT management, and to refine network and security architecture.

For additional information, contact Joe Re, CA2, (703) 882-2169, DSN 381.

Information Assurance (IA) Transformed

by Danielle Paolucci, CIAE

Many new Information Assurance (IA) challenges have surfaced as a result of the DoD transformation and because of changes in technology. These challenges require the transformation of many of the things DISA and DoD do in IA. Some of them are:

- Improved protection of key DoD critical infrastructures. The Chief Information Assurance Executive (CIAE) is responsible for the oversight of the Defense Information Infrastructure (DII) and Command, Control, and Communications sectors of DoD's Critical Infrastructure Protection (CIP) program. This includes responsibility for planning, coordination, and oversight of the two sectors for all the Combatant Commanders, military services and agencies, other than the intelligence community.

- Integrated operations across all technologies in the joint war-fighting process. DISA's goal is to enhance its existing secure sharing of network, computing, and cyber-attack status information with the military services/Combatant Commanders. To ensure each geographic Combatant Commander has integrated views of key joint warfighting information processes within the Combatant Commander's theater, and has awareness of attack/defense status throughout the Global Information Grid (GiG), as an extension to the Regional Network Operations and Security Centers (RNOSC), the Combatant Commander Network Operations and Security Capability (CNOSC), will provide an end-to-end global view of Network Operations (NETOPs) that impact the Combatant Commander GIG Area of Responsibility (AOR).

- Improved combined joint IA command and control/situational awareness. DISA efforts will improve modeling, visualization, and sharing of information about the warfighting information processes. As these capabilities are deployed and the raw data is shared, the rules for building a business process viewed from the data result in a fused IA picture. DISA will work with the rest of DoD to develop standards for interoperability and secure sharing of this data; much of this will be done via Advanced Concept Technology Demonstrations (ACTD).

- Improved agility of a joint or combined joint deployed force by fielding "plug-in" protections and detection systems in the sustaining infrastructure. In coordination with geographic Combatant Commanders, DISA is building a perimeter defense and intrusion detection capability at each Standardized Tactical Entry Point (STEP), and will operate the tools on behalf of Combatant Commanders and deployed (combined) joint task forces (JTF).

- Dynamic Counterintelligence Monitoring. This effort uses commercial tools to simultaneously monitor access to many crucial systems in order to detect patterns of misuse. This could enable the rapid formation of communities-of-interest in spite of possibly weak information protection methods; if misuse by a community member is detected, access can be quickly denied.

- Enhanced Vulnerability Management. Transformation efforts to combat complexity of systems and increased frequency of intervention include the gold disk program, a DoD-wide license for joint automated configuration management tools, and the deployment of tools to help find sophisticated site vulnerabilities. The gold disk provides a more automated way to secure a system by allowing replication of many identical, secure configurations, and reloading secure configurations; and for very high security applications, a secure starting point for adding more stringent security measures.

- Improved DoD Intranet/DMZ/web server/Internet access architecture. DISA is working with the rest of DoD to improve the unclassified network architecture by defining clear locations for publicly visible servers, standardizing a DoD-wide perimeter defense policy, and strengthening the DISA managed gateways to the Internet. DISA has a prototype server zone, called a demilitarized zone (DMZ), operating at the Defense Enterprise Computing Center (DECC) Columbus, and is working with the Defense Logistics Agency (DLA) to move many DoD electronic commerce systems into the DMZ.

The CIAE is committed to bringing new and innovative ideas and solutions to the forefront of the DISA IA program, and to work toward a common goal with the DoD-wide IA community. With a small core office, the CIAE works with other elements of DISA working IA issues, as well as working with others in DoD to ensure that DISA, as a team, delivers an effective IA effort to support our warfighting customers. Information about specific IA efforts is provided in regularly scheduled program reviews. The DoD Information Assurance Support Environment (IASE) website (http://iase.disa.mil/) is a valuable source for information.

For additional information, contact Danielle Paolucci, CIAE, (703) 882-1531, DSN 381.

A Warfighter's Definition

"Information Assurance Means

Assured Mission Execution"

LTG Burnette

Former Deputy Commander in Chief, Joint Forces Command

Securing NIPRNet Remote Network Management

by CDR Keith Fuller, API3

DISA provides the warfighter a long-haul transport service for both in-garrison and deployed network segments. To do so, DISA must establish protection mechanisms that match the potential level of threat to network resources and network level communications.

This requires maintaining a high-level of NIPRNet security to protect all DoD classified and unclassified sensitive information, and the communications components that process this information. To ensure the long-haul transport is available to meet demands, DISA's network security engineering approach is to harden network management and control infrastructure, and services used within the Defense Information System Network (DISN).

The ability to securely manage network devices and components is fundamental to this approach. DISA chose specific technologies for securing remote access sessions between management clients and network devices, as well as the relationships between remote access technology and methods of access required to manage the NIPRNet from the Network Operations Center (NOC).

The following approach, based on available technologies and the present management techniques used by DISA on the NIPRNet, was adopted to provide security protection for remote network management. The implementation process listed below is being executed in three phases, and is being conducted during a nine month period. The phases are:

Phase 1: Encrypt remote access session data.

Phase 2: Employ Authentication, Authority and Accounting (AAA) services.

Phase 3: Implement Strong User Authentication.

Phase 1: Encrypt Remote Access Session Data -- The most obvious security weakness in the current NIPRNet remote management methodologies is found in the "clear text" Telnet sessions from the workstations to the network devices. The Telnet protocol will be replaced with one that encrypts the session traffic; Secure Shell (ssh) was selected. Secure Shell products offer Digital Encryption Standard (DES) and 3DES encryption and use ssh's protocols to establish encrypted sessions over the network.

A tunnel-like encrypted session is immediately established during the connection process before the username and password information is put in. This guarantees that all critical data is encrypted during the management session, offering a significant security improvement over the existing methodology.

Currently, there are two implementations of "ssh" however, the two versions are incompatible with each other. Although Version 2 offers improved security through the support of 3DES, it is not supported in the current NIPRNet environment since the Cisco network devices only offer server support for Version 1. However, Cisco's implementation does include some proprietary adaptations and support for 3DES is offered in current versions of Cisco's router integrated operating system (IOS).

Phase 2: Employ AAA Services -- Many NIPRNet sites are now using some degree of Authentication, Authority and Accounting (AAA) services provided by Cisco System's CiscoSecure Access Control System (ACS) authentication server. The CiscoSecure ACS system can be implemented in support of authentication using either the TACACS+ or RADIUS protocol. The increased dependency for critical information transfer on today's networks attracts many perpetrators with access to sophisticated tools and utilities that can compromise network security.

The NIPRNet environment is predominantly managed via the Telnet protocol and incorporates basic user authentication (username and password matching) and, in some instances, AAA services provide additional authorization and accounting functionality. These Telnet sessions established across the network are comprised of "plain text" transmissions from the NOC workstation to the accessed network device.

The plain text transmission contains all of the user's keystrokes including username, password, device addresses, and input commands in plain view of someone who is able to capture the data traversing the network. This information in the wrong hands can be used maliciously to view the contents of a network device, and also to compromise the data and stop network operations. TACACS+ is the preferred choice because it provides more data protection and additional leverage for authorization parameters. TACACS+ can be applied to Telnet, FTP, and HTTP services at all network devices to prevent unauthorized network access.

Authentication services will be configured to provide the first tier of protection by confirming the validity of the username and password, based on a database entry managed by local administrators. Secondly, the authorization services will be configured to assign specific access rights and privileges to the network device. Finally, accounting services will be configured to provide a log of all user access information identifying who accessed the network device, when it was accessed, and what events occurred during the access.

Phase 3: Implement Strong User Authentication -- Because the NIPRNet environment currently requires username and password authentication, the addition of a second tier of authentication can easily be included to provide two-factor, strong user authentication functionality to network management. The planned candidate for this additional functionality is token server technology providing a continuously changing password/PIN for user authentication used with the typical username and password functions.

The token server technology requires a username and password match and a token server password match between a hardware token card in the user's possession and a database entry in a token server. The token technology incorporates a regularly expiring

one-time only password that deters a hacker from gaining access to an account by deriving the user's password.

RSA Security's SecurID ACE/Server System is the application used to provide this technology to the NIPRNet environment because of its widespread use today in the DISN ATM Service (DATMS). With the RSA Security solution for strong user authentication, authorized users are issued individually registered devices generating single-use token codes, which change based on a time code algorithm. Every 60 seconds, a different token-code is generated. The authentication server that protects the network validates this changing code. Each authentication device is unique and it is impossible to predict the value of a future token-code by recording prior token-codes. When a correct token-code is supplied, there is a high degree of certainty that the person is the valid user in possession of the RSA Security Authenticator.

A comprehensive network security engineering approach has been chosen by DISA to ensure the security of remote network management of the NIPRNet network devices. The application of an individual solution is less effective than the security resulting from the pairing of two or more technical solutions.

The effective implementation of these particular security technologies requires that these solutions be applied across the entire enterprise using a defense-in-depth approach. This approach will ensure optimum protection for remote network management, by protecting the host, network, data, and communication link, thus ensuring the long-haul transport is available to meet all the warfighter's demands.

For additional information, contact CDR Keith Fuller, API3, (703) 882-0448, DSN 381.

DISA Responds to Customer Requests with "Encore" Contracts

by Joe Myers, AQ13

DISA has awarded a third set of follow-on contracts to its popular Defense Enterprise Integration Services (DEIS) I and II procurements. The new contracts, called "Encore," incorporate a number of advancements from its predecessors and are focused on meeting the critical Information Technology (IT) needs of today and the future.

Encore provides IT solutions at attractive rates. Eleven task areas provide coverage of the wide IT's spectrum products and services. Sixty-five labor categories, which can be expanded, ensure that the customer is provided the exact talent needed at a low cost. In addition to establishing maximum labor rates, provisions of the contracts allow the contractors to propose lower rates during task order negotiations. Requirements may be stated either in terms of traditional task descriptions, or in performance-based work statements.

A team of IT industry leaders supports Encore, including ASI, CSC, EDS, Lockheed Martin, Northrop Grumman, Pragmatics Inc., TranTech, TRW, and UNISYS. Subcontractor support is comprised of more than 250 large, small, and small disadvantaged businesses. An appealing feature of Encore allows subcontractors to work under any prime for flexible customer teaming arrangements. Additionally, Encore is a seven-year contract that provides extended stability over traditional contracts.

The multiple-award, "fair opportunity" streamlining aspects of Encore significantly reduce standard lead-times. An automated past performance system greatly assists in awarding new task orders, cutting down time and effort. The web has replaced electronic mail providing for easier distribution and processing of proposals/awards. To further reduce processing, the Acquisition Planning and Execution (APEX) tool will support Encore. APEX is a web-based system that allows users to electronically develop, save and/or print a complete contract requirements package.

Responding to the military services, Defense Agencies, U.S. Allies and other Federal, state, and local governments, DISA's Acquisition, Logistics, and Facilities Directorate (AQ) is ready to satisfy requirements through Encore. A world of IT acquisition awaits you at **ACQuireIT**.

For additional information contact Joe Myers, AQ13, (618) 229-9392, DSN 779 or go to:

http://www.disa.mil/D4/diioss/.

Network Warfare Simulation (NETWARS)

by Greg Giovanis, TS3

DISA continues the successful partnership with the J-6 on NETWARS. A formal MOA was signed between Lt Gen Raduege and Lt Gen Woodward in July 2000 that assigned DISA software development responsibilities for the program.

NETWARS is the joint communications model and is currently in use by Services, Combatant Commanders and Agencies. It supports two broad communities of users. First, it allows Joint Task Force (JTF) communications planners the ability to coordinate and analyze requirements for deploying communications for real world operations. Second, it supports the analysis of communications requirements for changes in technology, applications, policy and doctrine.

The use of Commercial-off-the-Shelf (COTS) technology and a set of standards allows interoperability between an extensive set of communications device models developed by, and for, commercial communications vendors and models of military unique communications devices developed by DoD.

Network topologies are represented in terms of military organizations and network traffic is represented in terms of information exchange requirements (IERs). These representations allow an analyst to think in terms of how communications affect the accomplishment of military mission.

NETWARS is an evolutionary program and the Phase III Evolutionary Phased Implementation Plan is out for coordination. The evolutionary process focuses on a continuous interaction with users. After a requirement is identified, the program works with the user to map out exact functionality and the user interface. The design produced from this interaction is used to develop beta software that is taken to the user along with a workflow process. The comments from this are used to create production software. This process normally takes six months.

The main requirements for additional functionality come from the NETWARS Studies Advisory Group, comprised of O-6 and GS-15 level analysts from the stakeholder organizations. The intent is to only build new functionality into NETWARS that supports DoD's joint analysis requirements.

NETWARS successfully completed a validation study in April 2002. This analysis focused on Operation Enduring Freedom and examined how the networks supported the information flows required by a set of critical C4I applications. Tasks currently underway using NETWARS include, 1) an evaluation of the GCCS Korea (GCCS-K) current and future network performance considering an asynchronous transfer mode (ATM) backbone using encryption devices, and includes the impact of unmanned aerial vehicle (UAV) communications requirements; 2) an examination of the communications congestion at Navy telecommunications facilities and network operation centers as networks are migrated from legacy systems to the internet protocol (IP); 3) an assessment of the performance of the proposed Army's Interim Brigade Combat Team's (IBCT) Command and Control network in representative benign and hostile environments; and 4) the development and assessment of a new SOUTHCOM communications architecture and an evaluation of the impact of critical high bandwidth applications on the existing network.

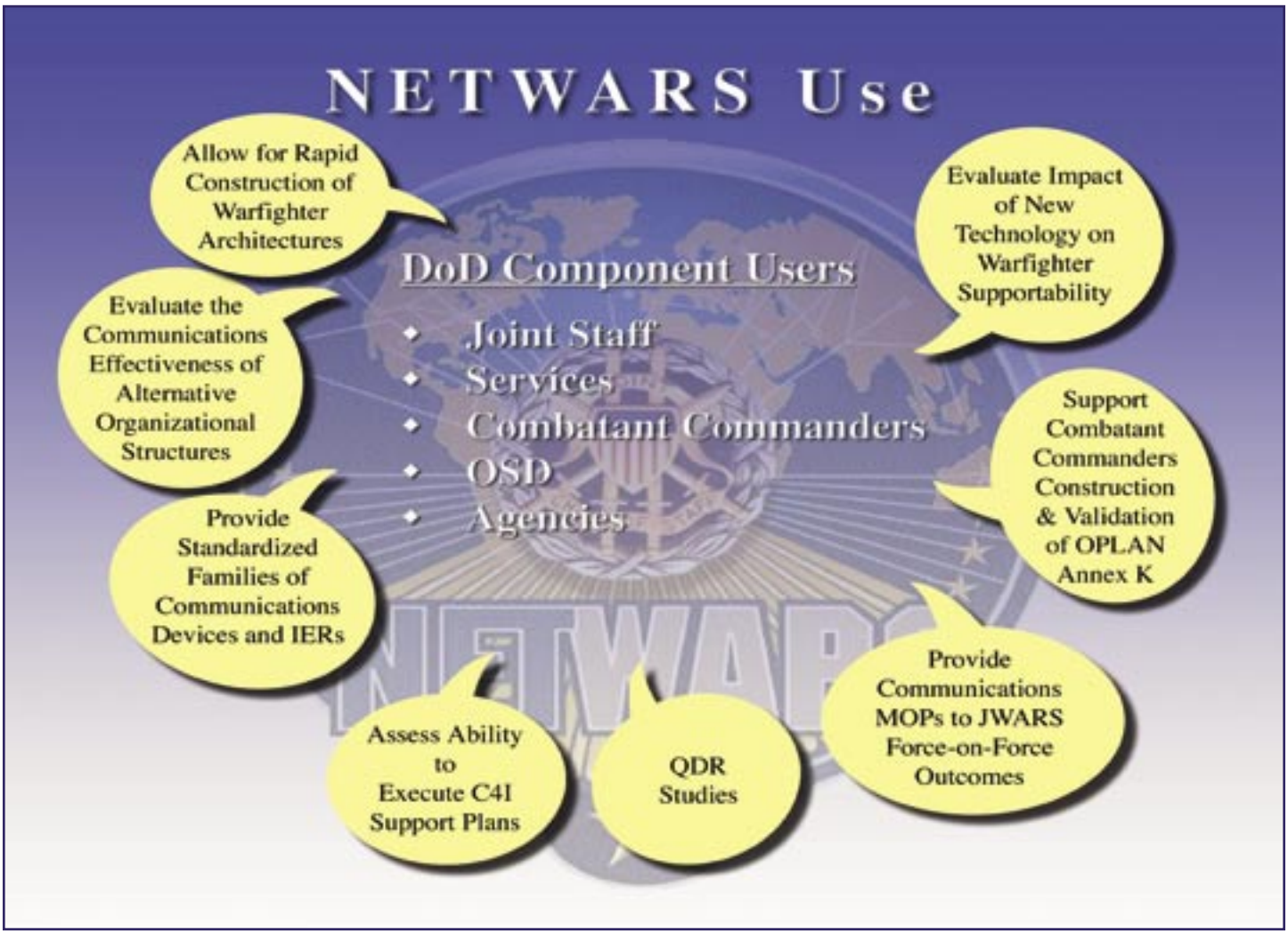
NETWARS provides communications data for the DoD Joint

Warfare Model (JWARS). NETWARS will be integrated into the Joint Network Management System (JNMS) as the JNMS's communications modeling tool.

NETWARS is a tool that will assist decision makers. For example, it will assist with acquisition decisions attempting to evaluate communications performance in a Network Centric Warfare paradigm or by quantifying the communications benefits of introducing new technologies or concepts of operation. It will assist communications planners in deploying more effective networks in support of military actions. In addition, it will assist communications operators by quantifying the impact of policy changes or reallocation of resources.

For additional information, contact Greg Giovanis, TS3, (703) 882-1802, DSN 381.

The Pacific Ocean, June 3, 2000 — Electronic Warfare Technician 3rd Class Michael Eubanks, from Dallas, TX, operates part of the Advanced Combat Direction Systems (ACDS) in the Electronic Warfare (EW) Module aboard USS Kitty Hawk (CV-63). U.S. Navy photo by Photographer's Mate 3rd Class Chris D. Howell.



DEFENSE INFORMATION SYSTEMS AGENCY

CUSTOMER ADVOCACY

The Voice For The Warfighter

Personal Zone: In Step with DISA Personnel

by Tannikka Richardson, CA4

From summer-hire to intern, this employee is doing it all…

Meet Catreena Walker. She works in DISA's Office of the Chief Financial Executive, where she balances work, school, motherhood and customer satisfaction. The second-year intern came to DISA five years ago as a summer-hire.

Catreena is a Danville, VA native and attended St. Paul's College in Lawrenceville, VA. She changed her focus of study in college when she discovered that she had the opportunity to work for DISA as a summer-hire/stay-in-school employee. While completing her Bachelor of Science degree in Accounting at George Mason University, she realized that coming to DISA was a wise decision. She watched fellow accounting majors work for "big five" accounting firms that were not sensitive to their academic curriculum. Catreena, on the other hand, had the opportunity to do work that supplemented her classroom experiences with team members who valued and supported her educational goals.

Upon graduating from George Mason, Catreena joined the DISA Intern Program, which gave her the opportunity to use the skills she learned as an undergraduate to help achieve DISA's customer focus, and at the same time pursue a Master of Science degree in Computer Information Systems from the University of Phoenix. She claims that the online study program takes discipline to accomplish, but it is ideal for her schedule while raising her 10-month old daughter, Mychala. When asked about her hobbies and interests, she smiled and said: "Who has time?" She mentioned that she enjoys get-togethers with friends and family.

Although she values the present, she has a sharp eye toward the future preparing to graduate from the Intern Program and from graduate school within months of each other.

For additional information, contact Tannikka Richardson, CA4, (703) 882-1924, DSN 381.